IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TYRONE MERRITT, JOSEPH ROYAL, JR., and JOHN SPACEK, individually and as representatives of the class, Plaintiff, vs. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., and CAPITAL ONE BANK (USA), Defendants.	**Case No: _____** **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Tyrone Merritt, Joseph Royal, Jr., and John Spacek (collectively "plaintiffs"), individually and on behalf of the class set forth below, bring this class action complaint against defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA) (collectively "Capital One"):

PRELIMINARY STATEMENT

1. This case is about one of the largest data security breaches in history, affecting millions of consumers who have entrusted their confidential personal and banking information to Capital One.

2. As a result of this breach, the plaintiffs and the class members whose personal information was not safeguarded now face substantial risk of further injury from identity theft, credit and reputational injury, false tax claims, or even extortion.

3. On July 29, 2019, Capital One publicly acknowledged that it was subject to one of the largest data breaches in history.

4. The data security breach disclosed the personal information related to approximately 100 million Capital One accounts.

5. The information stolen in the breach includes names, mailing addresses, telephone numbers, email addresses, Social Security numbers, dates of birth, credit histories, and portions of credit card customer data.

6. As a result of Capital One's failure to protect its customers' sensitive information, the plaintiffs and class members have been exposed to fraud, identity theft, and financial harm, as detailed below, and are subject to a heightened, imminent risk of such harm in the future.

7. The plaintiffs seek redress individually, and on behalf of those similarly-situated, for the injuries sustained as a result of Capital One's negligent and intentional violations of law.

8. The plaintiffs assert these claims on behalf of a nationwide class of Capital One customers for monetary relief, injunctive relief, corresponding

declaratory relief, and other appropriate relief for Capital One's unlawful conduct, as described herein.

PARTIES

9. Plaintiff Tyrone Merritt is a Maryland citizen residing in Port Republic, Calvert County, Maryland. His personal information was compromised in the data breach after providing it to Capital One in connection with applying and opening an account for a Capital One Platinum MasterCard. Upon information and belief, the following personal information of plaintiff Merritt was disclosed in the hack: name; address; phone number; email address; date of birth; and self-reported income. Plaintiff Merritt's Social Security number and additional credit card number data may also have been compromised.

10. Plaintiff Joseph Royal, Jr., is a Virginia citizen residing in Ashland, Hanover County, Virginia. His personal information was compromised in the data breach after providing it to Capital One in connection with applying and opening an account for a Capital One credit card. Upon information and belief, the following personal information of plaintiff Royal was disclosed in the hack: name; address; phone number; email address; date of birth; and self-reported income. Plaintiff Royal's Social Security number and additional credit card data may also have been compromised.

11. Plaintiff John Spacek is a Virginia citizen residing in Richmond, Virginia. His personal information was compromised in the data breach after providing it to Capital One in connection with applying and opening an account for a Capital One Venture credit card. Upon information and belief, the following personal information of plaintiff Spacek was disclosed in the hack: name; address; phone number; email address; date of birth; and self-reported income. Plaintiff Spacek's Social Security number and additional credit card data may also have been compromised.

12. Defendant Capital One Financial Corporation, a bank holding company, is ranked as one of the 10 largest banks in the United States by assets. The bank has over 755 branches and 2,000 ATM machines. Capital One Financial Corporation specializes in credit cards, auto loans, banking, and savings accounts. Capital One Financial Corporation is third largest credit card issuer and second largest auto finance company in the United States. Capital One Financial Corporation is incorporated in Delaware, with its principal place of business in McLean, Fairfax County, Virginia. Capital One Financial Corporation may be served with process upon its registered agent Corporation Service Company, 100 Shockoe Slip (Floor 2), Richmond, VA 23219.

13. Defendant Capital One, N.A., one of Capital One Financial Corporation's two principal subsidiaries, also maintains its principal place of business in McLean, Fairfax County, Virginia. It offers a broad spectrum of banking products and financial services to consumers, small business, and commercial clients. Capital One, N.A., may be served with process upon its registered agent Corporation Service Company, 100 Shockoe Slip (Floor 2), Richmond, VA 23219.

14. Defendant Capital One Bank (USA), one of Capital One Financial Corporation's two principal subsidiaries, also maintains its principal place of business in McLean, Fairfax County, Virginia. It offers a broad spectrum of credit and debit products to consumers. Capital One Bank (USA) may be served with process upon its registered agent Corporation Service Company, 100 Shockoe Slip (Floor 2), Richmond, VA 23219.

15. Defendant Capital One Financial Corporation operates primarily through defendants Capital One Bank (USA) and Capital One, N.A. As such, all Capital One defendants are jointly and severally liable for the harm complained of herein.

16. Upon information and belief, Capital One's wrongful acts and omissions leading to this data security breach occurred nationwide and in this district.

JURISDICTION & VENUE

17. This court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. Plaintiff Merritt, the class members, and defendant Capital One are citizens of different states. There are more than 100 putative class members.

18. This court has personal jurisdiction over the defendant because Capital One maintains its principal place of business in Virginia, regularly conducts business in Virginia, and has sufficient minimum contacts in Virginia.

19. Venue is proper in this court pursuant to 28 U.S.C. § 1391(a) because Capital One's principal place of business is in this district and a substantial part of the events, acts, and omissions giving rise to the plaintiff's claims occurred in this district.

FACTS

20. On July 29, 2019, Capital One confirmed "unauthorized access by an outside individual who obtained certain type of personal information relating to people who has applied for its credit card products and to Capital One credit card customers."

21. The confidential information was accessed on at least 23 occasions by Paige Thompson, a Seattle-area woman, who formerly worked at a cloud computing company that provided data services to Capital One. Thompson gained access to Capital One's sensitive customer data by exploiting a misconfigured web application firewall.

22. Capital One was oblivious to the problem until July 17, 2019, when Thompson, who went by the moniker "erratic" in online chats, made statements on social media to the effect that she had illegally taken large amounts Capital One's data. A person in an online discussion group brought the issue to Capital One's attention, and Thompson was later arrested by the FBI.

23. Capital One admitted that the compromised database contains sensitive information of over 100 million customers (an estimated 100 million in the United States and 6 million in Canada).

24. Capital One further acknowledged that "the largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income."

25. Beyond the credit card application data, Thompson also obtained portions of credit card customer data, including: (a) customer status data, e.g., credit scores, credit limits, balances, payment history, and contact information; and (b) fragments of transaction data from 23 days during 2016, 2017, and 2018.

26. Furthermore, approximately 140,000 credit card customers' Social Security numbers were taken, and approximately 80,000 credit card customers' bank account numbers were stolen. Approximately one million Canadians' Social Insurance Numbers were compromised.

27. Affected persons are those who, like the plaintiffs, provided information to obtain credit and/or open accounts with Capital One.

28. Capital One has a history of inadequate data security practices. In 2017, Capital One notified customers that a former employee had access for nearly four months to their personal data, including account numbers, telephone numbers, transaction history, and Social Security numbers. The company suffered a similar breach by an employee in 2014.

29. Additionally, Capital One was aware of numerous additional data hacks targeting the financial services industry, including Equifax (2017, 147 million accounts), Heartland Payment Systems (2008, 130 million accounts), TRW Information Systems (1984, 90 million accounts), JPMorgan Chase (2014, 83

million accounts), CardSystems Solutions (2005, 40 million accounts), Korea Credit Bureau (2014, 20 million accounts), Data Processors International (2003, 8 million accounts), CheckFree Corp. (2009, 5 million accounts), Citifinancial (2005, 3.9 accounts), Educational Credit Management Corp. (2010, 3.3 million accounts), Countrywide (2008, 2 million accounts), and Global Payments (2012, 1.5 million accounts).

30. Despite being a holder of sensitive personal information for millions of customers, Capital One failed to prioritize data security by adopting reasonable safeguards to prevent and detect unauthorized access to its customers' information. Capital One had ample resources to prevent a breach, but failed to prioritize data security while spending millions on executive compensation, marketing, and other endeavors.

31. Capital One's privacy policy, on information and belief disseminated to all its customers, provided its customers with a false sense of security with respect to the safety of their confidential personal information: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files in buildings." (*See* "Capital One Privacy And Opt-Out Notice" (accessed July 29, 2019), available at: https://www.capitalone.com/privacy/notice/en-us/).

32. Similarly, Capital One's Online and Mobile Privacy Statement erroneously promised customers: "At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices. (*See* "Capital One Online & Mobile Privacy Statement" (accessed July 29, 2019), available at: https://www.capitalone.com/identity-protection/privacy/statement).

33. Capital One also falsely pledged that its customers' Social Security numbers were safe: "Capital One protects your Social Security Number. Our policies and procedures: (1) Protect the confidentiality of Social Security numbers; (2) Prohibit the unlawful disclosure of Social Security numbers, and (3) Limit access to Social Security numbers to employees or others with legitimate business purposes. (*See* "Social Security Number Protections" (accessed July 29, 2019), available at: https://www.capitalone.com/identity-protection/privacy/social-security-number).

34. Capital One's conduct, as described above, demonstrates a willful and conscious disregard for consumer privacy.

35. As a result of Capital One's conduct, the plaintiffs and class members' sensitive and confidential personal information has been compromised. They are

now at heightened risk for a variety of crimes, including but not limited to the following: tax fraud, identity theft such as opening fraudulent credit cards and loan accounts; various types of government fraud, such as obtaining a driver's license in the victim's name, or procuring government benefits with the victim's information; or medical fraud, such as using the victim's information to submit false insurance claims, illicitly obtain prescription drugs, etcetera.

36. In addition, the plaintiffs and class members will have to deal with the repercussions of identity theft, which are time consuming and difficult to manage. These cots include not only theft of personal information, but costs associated with detection and prevention of identity theft and unauthorized use of accounts, such as the purchase of credit monitoring or similar services. Other costs include but are not limited to: lower credit scores resulting from credit inquiries following fraudulent activities; costs associated with time spent and the loss of productivity from taking time to address and mitigate the actual and future consequences of the data breach, such as increased monitoring of accounts, and canceling and reissuing cards; and continued risk of expose to the thieves who now have, and can sell, the victims' information.

37. The plaintiffs and class members will be dealing with the fallout of this hack for years. The United States Government Accountability Office reports:

> [L]aw enforcement officials told us that in some cases, **stolen data may be held for up to a year or more before being used to commit identity theft.** Further, once stolen data have been sold or posted on the Web, **fraudulent use of that information may continue for years.** As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out future harm.[1]

38. The plaintiffs bring this action on their own behalf as well as on behalf of all similarly situated Capital One customers.

39. The plaintiffs seek declaratory and injunctive relief to prevent the Capital One from continuing its unlawful conduct, and to recover damages and costs, including reasonable attorneys' fees, for the injuries that the plaintiffs and class members have sustained.

CLASS ACTION ALLEGATIONS

40. Plaintiffs Merritt, Royal, and Spacek, and the class members as defined below, have been damaged by Capital One's negligent or reckless disregard for their personal information.

41. The plaintiffs bring this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

[1] U.S. Gov't Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown (2007). (Emphasis supplied).

42. The plaintiffs assert the claims herein on behalf of a proposed Nationwide Class ("the Class") defined as follows:

> All persons whose information was made accessible in the data security breach announced by Capital One on July 29, 2019.[2]

43. Numerosity: The members of the class are so numerous that joinder of all class members is impracticable. More than 100 million Capital One customers are affected by the data security breach.

44. Typicality: The plaintiffs' claims are typical of other class members because, among other things, all class members were comparably injured by the Capital One's negligent, reckless, and intentional conduct, as described above, which caused the data security breach.

45. Adequacy: The plaintiffs will fairly and adequately protect the interests of the class. Furthermore, they have retained counsel experienced in class actions and complex litigation.

[2] The following are excluded from the class: (1) the Capital One defendants, their offices and directors, as well as their parent companies, subsidiaries and affiliates, legal representatives, and any co-conspirators; and (2) any judge or magistrate presiding over this action, and members of their families. The plaintiffs reserve the right to amend the class period and/or class definition if discovery and further investigation reveal that the class should be expanded, divided into additional subclasses, or modified in any way.

46. Commonality and Predominance: Common questions of law and fact exist as to all class members and predominate over any questions solely affecting individual members of the class, including but not limited to:

a) whether Capital One owed duties under federal or state law to class members to protect their personal information, and to provide meaningful and fair redress;

b) whether Capital One breached said duties;

c) whether Capital One acted wrongfully by improperly monitoring, storing, and/or failing to properly safeguard the class members' personal information;

d) whether Capital One knew, or reasonably should have known, about the deficiencies in its data storage systems;

e) whether Capital One willfully failed to design, employ, and maintain a system adequate to protect consumers' personal information;

f) whether Capital One's representations regarding the security of its systems were false and misleading;

g) whether Capital One's acts and omissions violated applicable state consumer protection law;

h) whether Capital One's failures resulted in the data security breach at issue; and

i) whether class members have been damaged and, if so, the appropriate relief.

47. This case is maintainable as a class action under Fed. R. Civ. P. 23(b)(2) because Capital One has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

48. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the class predominate over any questions affecting only individual members of the class, and because a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

49. Capital One's conduct as described in this complaint stems from common and uniform policies and practices.

50. The class members do not have an interest in pursuing separate individual actions against Capital One, as the amount of each class member's individual claims are small compared to the expense and burden of individual prosecution.

51. Class certification also will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning the defendant's practices. Moreover, management of this action as a class action will not present any likely difficulties. In the interests of justice and judicial efficiency, it would be desirable to concentrate the litigation of all class members' claims in a single forum.

52. The plaintiffs intend to send notice to all class members to the extent required by Rule 23.

CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE
(On behalf of the Nationwide Class)

53. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

54. Defendant Capital One was, and continues to be, in a confidential, special, and/or fiduciary relationship with the plaintiffs and the class members by virtue of being trusted with their personal information.

55. At the very least, Capital One assumed a duty, and had duties imposed upon it by regulations, to comply with applicable security standards, regulations, and statutes, and to otherwise use reasonable care to safeguard the plaintiffs' and the class members' personal information.

56. By its acts and omissions as described herein, Capital One unlawfully breached its duties to the plaintiffs and the class members, who were harmed as a direct result.

57. Capital One knew, or should have known, that its system for processing and storing class members' personal information was replete with security vulnerabilities.

58. Capital One was negligent by continuing to accept, process, and store such information in light of its computer system vulnerabilities and the sensitivity of the personal information stored therein.

59. The data security breach, and resulting damages suffered by the plaintiffs and the class members, were the direct and proximate result of a number of actions and omissions, including but not limited to:

(a) Capital One's improper retention and storage of the plaintiffs' and class members' personal information; and

(b) Capital One's failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect such information;

60. Capital One's wrongful actions, as described above, reflect a breach of the duty of reasonable care and, therefore, constitute negligence.

61. The plaintiffs and the class members have not in any way contributed to the data security breach or theft of their personal information.

COUNT II – NEGLIGENCE PER SE
(On behalf of the Nationwide Class)

62. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

63. Pursuant to the Graham-Leach-Bliley Act, 15 U.S.C. § 6801, the Federal Trade Commission Act, 15 U.S.C. § 45, and related state consumer data protection statutes, defendant Capital One had a duty to protect and keep consumers' personal information secure, private, and confidential.

64. Capital One violated these laws by not adequately safeguarding the plaintiffs' and class members' personal information, as well as by not ensuring that Capital One itself complied with applicable data security standards, card association standards, regulations, and/or statutes designed to protect such information.

65. Capital One's failure to comply with the Graham-Leach-Bliley Act, the Federal Trade Commission Act, industry standards, and state laws and regulations constitutes negligence *per se*.

COUNT III – BREACH OF FIDUCIARY DUTIES
(On behalf of the Nationwide Class)

66. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

67. Defendant Capital One, by virtue of its possession, custody, and/or control of the plaintiffs' and the class members' personal information, and Capital One's duty to properly monitor and safeguard said information, was, and continues to be, in a confidential, special, and/or fiduciary relationship with the plaintiffs and the class members.

68. As a fiduciary, Capital One owed, and continues to owe, the plaintiffs and the class members:

(a) the commitment to deal fairly and honestly;

(b) the duties of good faith and undivided loyalty; and

(c) integrity of the strictest kind.

69. Capital One was, and continues to be, obligated to exercise the highest degree of care in carrying out the responsibilities to the plaintiffs and class members under such confidential, special, and/or fiduciary relationships.

70. Capital One breached its fiduciary duties to the plaintiffs and the class members when it failed to adequately store, monitor, and protect the plaintiffs' and class members' personal information.

71. Capital One willfully and wantonly breached its fiduciary duties to the plaintiffs and class members or, at the very least, committed these breaches with conscious indifference and reckless disregard of the plaintiffs' and class members' rights and interests.

COUNT IV – BREACH OF CONTRACT
(On behalf of the Nationwide Class)

72. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

73. The plaintiffs and class members were parties to actual or implied contracts with defendant Capital One that required Capital One to properly safeguard their personal information from theft, compromise, and/or unauthorized disclosure.

74. Additionally, the plaintiffs and class members were third-party beneficiaries to contracts between Capital One and other entities under which the Capital One was required to safeguard its customers' personal information from theft, compromise, and/or unauthorized disclosure.

75. Capital One's wrongful acts as described herein constitute breaches of these contracts.

COUNT V – BAILMENT
(On behalf of the Nationwide Class)

76. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

77. The plaintiffs' and class members' personal information is their property, which they delivered to defendant Capital One for the sole and specific purpose of completing one or more commercial transactions.

78. Capital One accepted the plaintiffs' and class members' personal information and, thus, served as a bailee with respect to the above-referenced transaction(s).

79. Capital One, as bailee, owed a duty to the plaintiffs and class members and, in fact, had an express and/or implied contract with them to protect their personal information from theft, compromise, or unauthorized disclosure.

80. Capital One breached its duty and/or express and implied contracts with the plaintiffs and class members by improperly storing and inadequately protecting their personal information from theft, compromise, and/or unauthorized disclosure, which directly and proximately caused the plaintiffs and class members to suffer damages.

81. Capital One's wrongful actions constitute breaches of its duties (and/or express and/or implied contracts) with the plaintiffs and the class members arising from the bailment.

COUNT VI – UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

82. Plaintiffs Merritt, Royal, and Spacek, on behalf of the Class, allege and incorporate by reference the allegations in the preceding paragraphs.

83. The plaintiffs bring this cause of action on behalf of the class members and, to the extent necessary, in the alternative to their breach of contract claims.

84. The plaintiffs and class members conferred a monetary benefit on defendant Capital One in the form of money paid to Capital One for its services.

85. The plaintiffs and class members also provided their personal information to Capital One which Capital One then utilized for monetary purposes.

86. Capital One appreciated or had knowledge of the benefits conferred upon it by the plaintiffs and class members.

87. The money paid by the plaintiffs and class members to Capital One should have been used by Capital One, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

88. As a result of Capital One's conduct, the plaintiffs and class members suffered actual damages in an amount equal to the difference in value between services with reasonable data privacy and security practices and procedures that the

plaintiffs and class members paid for, and inadequate services without reasonable data privacy and security practices and procedures that they received.

89. Under principles of equity and good conscience, Capital One should not be permitted to retain the money belonging to the plaintiffs and class members because Capital One failed to implement adequate data privacy and security practices and procedures that the plaintiffs and class members paid for.

90. Capital One should be compelled to disgorge into a common fund all unlawful or inequitable proceeds it received, and a constructive trust should be placed upon such funds for the benefit of the plaintiffs and class members.

PRAYER FOR RELIEF

91. As a direct and proximate cause of defendant Capital One's wrongful conduct, plaintiffs Merritt, Royal, Spacek, and the class members sustained, and will continue to incur, damages in the form of:

a) the unauthorized disclosure and/or compromise of their personal information;

b) monetary losses and damage to credit from fraudulent charges made upon their accounts; and

c) the burden and expense of credit monitoring.

92. Accordingly, the plaintiffs, individually and on behalf of the Class,

request relief as follows:

a) certification of the Class pursuant to Fed. R. Civ. P. 23, as requested herein;

b) appointment of plaintiffs Merritt, Royal, and Spacek as class representatives, and the undersigned counsel as class counsel;

c) an order directing that reasonable notice of this action, as provided by Fed. R. Civ. P. 23(c)(2), be given to every class member;

d) equitable relief to prevent any additional harm including, but not limited to, provision of credit monitoring services for a time to be determined by a trier of fact;

e) an injunction permanently enjoining Capital One, as well as its subsidiaries and affiliates, from further engaging in the same acts or omissions that led to the data security breach described above;

f) a judgment in favor of the plaintiffs and class members under the legal theories alleged herein;

g) an award to the plaintiffs and class members of nominal damages, compensatory damages, and/or punitive damages, to the extent allowed by law;

h) an award to the plaintiffs and class members of restitution and/or disgorgement of profits;

i) an award to the plaintiffs and class members of pre- and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of this complaint;

j) an award to the plaintiffs and class members of reasonable attorneys' fees, costs, and expenses; and

k) granting such other relief as the court deems just and proper.

DEMAND FOR JURY TRIAL

93. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, the plaintiffs and class members demand a trial by jury.

Respectfully submitted August 9, 2019.

GEOFF McDONALD & ASSOCIATES, P.C.

/s/ Geoffrey R. McDonald
GEOFFREY R. McDONALD (VSB No. 30544)
JUSTIN M. SHELDON (VSB No. 82632)
FRANK H. HUPFL (VSB No. 82972)
3315 West Broad Street
Richmond, VA 23230
Tel: (804) 888-8888
Fax: (804) 359-5426
GMcDonald@mcdonaldinjurylaw.com
JSheldon@mcdonaldinjurylaw.com
FHupfl@mcdonaldinjurylaw.com

BEASLEY, ALLEN, CROW, METHVIN, PORTIS & MILES, P.C.

/s/ W. Daniel "Dee" Miles, III
W. DANIEL "DEE" MILES, III*
ARCHIE I. GRUBB, II*
LESLIE L. PESCIA*
218 Commerce Street
Montgomery, AL 36104
Tel: (334) 269-2343
Fax: (334) 954-7555
Dee.Miles@BeasleyAllen.com
Archie.Grubb@BeasleyAllen.com
Leslie.Pescia@BeasleyAllen.com

** To be admitted pro hac vice*